FSA Certification and Accreditation (C&A) Package Submission Process

As you know the Department is undertaking an important and ambitious effort to certify and accredit the security posture of our major IT systems. The Department's commitment is to certify and accredit a number of IT systems by 9/30/03 and the rest of our major IT systems by 12/31/03.

The ED CIO, Bill Leidenger, sent a memo last week to ED Principal Offices that described the C&A Package Submission Process. The memo contained procedures that do not apply to FSA. As a result, FSA system owners instead should disregard Attachment 2 of Mr. Leidinger's memo and follow the below FSA-specific procedures for submitting C&A packages.

This process is described in four (4) phases below.

PHASE I: PRE-CERTIFICATION REVIEW

Step 1 – Perform Initial Review. Systems will undergo a pre-certification review of C&A documentation prior to formal submission to the Certification Review Group (CRG). The purpose of this review is to assist system owners in solidifying the depth, accuracy, and compliance of their documentation. Security Test and Evaluation (ST&E) Plans will not be reviewed prior to submission to the CRG.

Specific Responsibilities:

- System Security Officers place most current C&A documentation into Public Folders
- ED OCIO reviews documentation and completes an Observation Matrix.

  >> Note: The matrix contains observations that have been categorized based on a color-coding scheme to depict the severity and impact of a particular observation (i.e., red – severe impact, yellow – potential impact, green – not a major issue but, addressing the observation will enhance the document)

Step 2 – Contact System Owners. Upon completion of C&A documentation review, system owners will be notified via a formal memo to inform them of the observations found during the system documentation review. System owners should correct "red" observations prior to submitting the applicable document to the CRG. If observations are not corrected prior to submitting documentation to the CRG, the system owner must create a corrective action plan indicating how and when the observation will be addressed. All "red" finding must be mitigated prior to the execution of the Security Test and Evaluation Plans by the CRG.

Specific Responsibilities:

- ED OCIO provides the Certifier (i.e., Bill Leidinger or Terri Shaw) with the Observation Matrix for each system
- In cases where C&A documentation contains red observations, the Certifier contacts the applicable system owner to discuss the urgency to quickly rectify these observations
- System owners submit a response to the Certifier stating their plan to address and correct red observations

Step 3 – C&A Documentation Revised. System owners modify their C&A documentation based on the observations and recommendations identified in the Observation Matrix.

Step 4 – System Security Officers Update Public Folders System Security Officers must update their public folder with the revised C&A documentation and notify FSA CSO (Robert Ingwalson) upon completion. FSA Security and Privacy team will create one (1) CD per system containing all C&A documentation (including required revisions from Step 2 above) for the applicable system by the due date provided in Attachment 1 and deliver to the COR (Charles Warner). The CD will be accompanied with a formal memo (See Attachment 3) signed by a senior official. The certifier will forward the documentation and the signed memo to charles.warner@ed.gov.

>> Note: If the system owner cannot make the required Step-2 revisions and still meet the required due date, then they must submit a Corrective Action Plan to the Certifier and cc FSA CSO. The Corrective Action Plan must state: What will be fixed (i.e., the observations described under Step 2), How it will be fixed, When it will be fixed, and Who will fix it. The system owner will coordinate with FSA CSO to ensure that the corrections are made before the CRG makes its certification recommendations for Tier 2 systems, or before the CRG begins performing ST&E testing for Tier 3 and 4 systems. The FSA CSO will inform ED OCIO when observations are mitigated. The FSA Security and Privacy team will submit this Corrective Action Plan along with the one (1) CD and signed memo to the certifier by the required due date from Attachment 1.

PHASE II: CERTIFICATION REVIEW GROUP DUTIES

Step 1 – COR provides the CRG with one CD per system containing C&A documentation for the particular system

Step 2 – CRG conducts an independent review of the system's C&A documentation

Step 3 – CRG creates VDC ST&E Plan and updates remaining FSA system ST&E Plans as necessary.

Step 4 - CRG performs vulnerability scans and penetration tests on Tier 4 systems.

Step 5 - CRG provides the system owner with an out-brief of its review findings.

Step 6 – CRG prepares certification recommendations based on documentation validation and ST&E and penetration test results, if applicable.

Step 7 – CRG provides certification recommendations to the Certifier

PHASE III: CERTIFICATION

The Certifier makes the certification decision and makes an accreditation recommendation to the senior officer who owns the system. The Certifier for FSA systems is Bill Leidinger. The Certifier for non-FSA systems is Terry Shaw.

Step 1 – The Certifier reviews the CRG's certification recommendation and evaluates all areas indicating areas of failed compliance.

Step 2 – The Certifier develops a Certification recommendation; either Certify or Do Not Certify

Step 3 – The Certifier creates and sends an official certification memo to send to the DAA with the certification recommendation.

PHASE IV: ACCREDITATION

The DAA for FSA systems is Terry Shaw.

Step 1 – The DAA receives the certification recommendation from the certifier.

Step 2 – The DAA makes one of three decisions: Approve the system to operate; Grant Interim Approval to Operate until deficiencies are corrected; Deny Accreditation

- If the decision is accreditation, then no further action is required.
- If the decision is non-accreditation, then the Senior Officer proceeds to correct deficiencies.

Step 3 – The DAA notifies the Certifier of the decision in an official memorandum.